(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 782 112 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.07.1997 Bulletin 1997/27

(51) Int. Cl.[6]: **G07B 17/04**

(21) Application number: **96120496.3**

(22) Date of filing: **19.12.1996**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **19.12.1995 US 575104**

(71) Applicant: **PITNEY BOWES INC.**
Stamford Connecticut 06926-0700 (US)

(72) Inventors:
- **Braun, John F.**
  Weston, CT 06883 (US)
- **Cordery, Robert A.**
  Danbury, CT 06811 (US)
- **Pintsov, Leon A.**
  West Hartford, CT 06117-1900 (US)

(74) Representative: **Avery, Stephen John et al**
Hoffmann, Eitle & Partner,
Patent- und Rechtsanwälte,
Arabellastrasse 4
81925 München (DE)

(54) Transaction evidencing system and method including post printing and batch processing

(57) A transaction evidencing system and method includes a host processor and an unsecured printer coupled to the host processor. A vault device that includes digital token generation and transaction accounting functions is operatively coupled to the host processor. The vault device generates a digital token in response to a first command from the host processor. The digital token and information relating thereto are stored in storage area in the vault and/or the host processor. The stored digital token and information relating thereto are selectively accessed for generating transaction evidencing indicia corresponding to the stored digital token. The unsecured printing structure prints the transaction evidencing indicia in response to a second command which is issued at a time subsequent to the first command. A batch of digital tokens may be generated and stored in an indexed file in the storage area before any indicia corresponding to the batch of digital tokens are generated and printed. The host processor may be a personal computer and the vault device may be a portable vault card that is removably coupled to the personal computer. The information related to the digital token is postal information including piece count, postage amount and addressee information and the indexed file is indexed according to addressee information.

EP 0 782 112 A2

Description

The present invention relates generally to value printing systems and, more particularly, to value printing systems wherein a printer is not dedicated to a metering module.

The present application is related to the following U.S. Patent Applications Serial Nos. [Attorney Dockets E-416, E-415, E-417, E-418, E-419, E-420, E-421, E-444, E-462 and E-466], each filed concurrently herewith, and assigned to the assignee of the present invention.

The United States Postal Service is presently considering requirements for two metering device types: closed systems and open systems. In a closed system, the system functionality is solely dedicated to metering activity. Examples of closed system metering devices, also referred to as postage evidencing devices (PEDs), include conventional digital and analog postage meters wherein a dedicated printer is securely coupled to a metering or accounting function. In a closed system, since the printer is securely coupled and dedicated to the meter, printing cannot take place without accounting. Recently, Pitney Bowes Inc. has introduced the Post Perfect™ meter which is a new closed system metering device that includes a dedicated digital printer securely coupled to a secure accounting module.

In an open system, the printer is not dedicated to the metering activity, freeing system functionality for multiple and diverse uses in addition to the metering activity. Examples of open system metering devices include personal computer (PC) based devices with single/multi-tasking operating systems, multi-user applications and digital printers. An open system metering device is a PED with a non-dedicated printer that is not securely coupled to a secure accounting module.

When a conventional PED prints a postage indicia on a mailpiece, the accounting register within the PED must always reflect that the printing has occurred. Postal authorities generally require the accounting information to be stored within the postage meter in a secure manner with security features that prevent unauthorized and unaccounted for postage printing or changes in the amounts of postal funds stored in the meter. In a closed system, the meter and printer are integral units, i.e., interlocked in such a manner as to ensure that the printing of a postage indicia cannot occur without accounting.

Since an open system PED utilizes a printer that is not used exclusively for printing proof of postage payment, additional security measures are required to prevent unauthorized printing evidence of postage payment. Such security measures include cryptographic evidencing of postage payment by PEDs in the open and closed metering systems. The postage value for a mail piece may be encrypted together with other data to generate a digital token. A digital token is encrypted information that authenticates the information imprinted on a mail piece including postage values.

Examples of systems for generating and using digital tokens are described in U.S. Patents Nos. 4,757,537, 4,831,555, 4,775,246, 4,873,645, and 4,725,718, the entire disclosures of which are hereby incorporated by reference. These systems employ an encryption algorithm to encrypt selected information to generate at least one digital token for each mailpiece. The encryption of the information provides security to prevent altering of the printed information in a manner such that any misuse of the tokens is detectable by appropriate verification procedures.

Typical information which may be encrypted as part of a digital token includes origination postal code, vendor identification, data identifying the PED, piece count, postage amount, date, and, for an open system, destination postal code. These items of information, collectively referred to as Postal Data, when encrypted with a secret key and printed on a mail piece provide a very high level of security which enables the detection of any attempted modification of a postal revenue block or a destination postal code. A postal revenue block is an image printed on a mail piece that includes the digital token used to provide evidence of postage payment. The Postal Data may be printed both in encrypted and unencrypted form in the postal revenue block. Postal Data serves as an input to a Digital Token Transformation which is a cryptographic transformation computation that utilizes a secret key to produce digital tokens. Results of the Digital Token Transformation, i.e., digital tokens, are available only after completion of the Accounting Process.

Digital tokens are utilized in both open and closed metering systems. However, for open metering systems, the non-dedicated printer may be used to print other information in addition to the postal revenue block and may be used in activity other than postage evidencing. In an open system PED, addressee information is included in the Postal Data which is used in the generation of the digital tokens. Such use of the addressee information creates a secure link between the mailpiece and the postal revenue block and allows unambiguous authentication of the mail piece.

In conventional postage metering devices the printing and accounting for postage has been tightly coupled, both in time and proximity. For example accounting and printing takes place at virtually the same time as printing and in the same physically secure housing. Such coupling of the printing and accounting operations provides a high level of security for each transaction. Forensic methods have been devised for assuring that the indicia image was produced by a conventional postage metering device.

It has been discovered that in a PC-based meter system the meter vault can generate open system digital tokens that can be stored for the generation and printing of indicia at a later time. It has been discovered that in the open metering systems the printing and accounting functions can be physically separated because the security is not in the device but in the des-

tination address code included in the digital token calculation. The present invention takes advantage of this aspect of the open metering system to provide a system and method for generating one or more batches of addressee related digital tokens, storing them in a file and later generating and printing indicia therefrom at a later time, for example, seconds or days later.

An open metering system comprises a vault, a user interface and printer. In the present invention, the user interface is a standard PC. Users enter or store addresses on their PC. When a user desires to print an envelope, a message is sent to the vault requesting postage for a particular address and date (usually the current date). The vault performs appropriate postal accounting procedures, generates digital tokens and other indicia information and communicates them to the PC. The PC then sends a message to the printer which prints the envelope. This present invention improves this process by storing the information received from the vault in a PC file (in RAM or on disk) for printing at a later time.

The process to generate any number of mailpieces in accordance with the present invention proceeds in much the same manner as described above. A user enters the address or list of addresses (or recalls them from a file on disk) and the intended date of submission to the Post (usually defaulting to the current date). The PC then requests postage for all of the entered addresses. The vault performs the appropriate postal accounting procedures, generates digital tokens and the other indicia information and communicates them to the PC. The PC then stores them either in RAM or in non-volatile memory (such as a hard disk). They may then be printed immediately or at anytime in the future. This allows a user to generate tokens and format envelopes which will be mailed at a predetermined future date. The user may then print these envelopes at any time before that date. In addition, the envelope(s) may be previewed by the user prior to printing. At this time the user may change or add any non-postal related information to the envelope. Examples information which may be changed added are: ad slogans, return addresses, tag lines, etc.

In accordance with the present invention, a transaction evidencing system and method includes a host processor and an unsecured printer coupled to the host processor. A vault device that includes digital token generation and transaction accounting functions is operatively coupled to the host processor. The vault device generates a digital token in response to a first command from the host processor. The digital token and information relating thereto are stored in storage area in the vault and/or the host processor. The stored digital token and information relating thereto are selectively accessed for generating transaction evidencing indicia corresponding to the stored digital token. The unsecured printing structure prints the transaction evidencing indicia in response to a second command which is issued at a time subsequent to the first command. A batch of digital tokens may be generated and stored in an indexed file in the storage area before any indicia corresponding to the batch of digital tokens are generated and printed. The host processor may be a personal computer and the vault device may be a portable vault card that is removably coupled to the personal computer. The information related to the digital token is postal information including piece count, postage amount and addressee information and the indexed file is indexed according to addressee information.

The above and other objects and advantages of the present invention will be apparent upon consideration of the following detailed description, taken in conjunction with accompanying drawings, in which like reference characters refer to like parts throughout, and in which:

Fig. 1 is a block diagram of a PC-based metering system in accordance with the present invention;
Fig. 2 is a schematic block diagram of the PC-based metering system of Fig. 1 including a removable vault card and a DLL in the PC;
Fig. 3 is a schematic block diagram of the DLL in the PC-based metering system of Fig. 1 including interaction with the vault to generate indicia bitmap;
Fig. 4 is a block diagram of the DLL sub-modules in the PC-based metering system of Fig. 1;
Fig. 5 is a block diagram showing the difference between transaction processing in a conventional postage and the PC-based metering system of Fig. 1;
Fig. 6 is a flow chart of the batch processing of digital tokens; and
Fig. 7 is a flow chart of an alternate batch processing of digital tokens.

In describing the present invention, reference is made to the drawings, wherein there is seen in Figs. 1-4 an open system PC-based postage meter, also referred to herein as a PC meter system, generally referred to as 10, in which the present invention performs the digital token process. PC meter system 10 includes a conventional personal computer configured to operate as a host to a removable metering device or electronic vault, generally referred to as 20, in which postage funds are stored. PC meter system 10 uses the personal computer and its printer to print postage on envelopes at the same time it prints a recipient's address or to print labels for pre-addressed return envelopes or large mailpieces. It will be understood that although the preferred embodiment of the present invention is described with regard to a postage metering system, the present invention is applicable to any value metering system that includes a transaction evidencing.

As used herein, the term personal computer is used generically and refers to present and future microprocessing systems with at least one processor operatively coupled to user interface means, such as a display and keyboard, and storage media. The personal computer may be a workstation that is accessible by

more than one user.

The PC-based postage meter 10 includes a personal computer (PC) 12, a display 14, a keyboard 16, and an non-secured digital printer 18, preferably a laser or ink-jet printer. PC 12 includes a conventional processor 22, such as the 80486 and Pentium processors manufactured by Intel, and conventional hard drive 24, floppy drive(s) 26, and memory 28. Electronic vault 20, which is housed in a removable card, such as PCMCIA card 30, is a secure encryption device for postage funds management, digital token generation and traditional accounting functions. PC meter system 10 may also include an optional modem 29 which is located preferably in PC 12. Modem 29 may be used for communicating with a Postal Service or a postal authenticating vendor for recharging funds (debit or credit). In an alternate embodiment the modem may be located in PCMCIA card 30.

PC meter system 10 further includes a Windows-based PC software module 34 (Figs. 3 and 4) that is accessible from conventional Windows-based word processing, database, accounting and spreadsheet application programs 36. PC software module 34 includes a vault dynamic link library (DLL) 40, a user interface module 42, and a plurality of sub-modules that control the metering functions. DLL module 40 securely communicates with vault 20 and provides an open interface to Microsoft Windows-based application programs 36 through user interface module 42. DLL module 40 also securely stores an indicia image and a copy of the usage of postal funds of the vault. User interface module 42 provides application programs 36 access to an electronic indicia image from DLL module 40 for printing the postal revenue block on a document, such as an envelope or label. User interface module 42 also provides application programs the capability to initiate remote refills and to perform administrative functions.

Thus, PC-based meter system 10 operates as a conventional personal computer with attached printer that becomes a postage meter upon user request. Printer 18 prints all documents normally printed by a personal computer, including printing letters and addressing envelopes, and in accordance with the present invention, prints postage indicia.

The vault is housed in a PCMCIA I/O device, or card, 30 which is accessed through a PCMCIA controller 32 in PC 12. A PCMCIA card is a credit card size peripheral or adapter that conforms to the standard specification of the Personal Computer Memory Card International Association. Referring now to Figs. 2 and 3, the PCMCIA card 30 includes a microprocessor 44, redundant non-volatile memory (NVM) 46, clock 48, an encryption module 50 and an accounting module 52. The encryption module 50 may implement the NBS Data Encryption Standard (DES) or another suitable encryption scheme. In the preferred embodiment, encryption module 50 is a software module. It will be understood that encryption module 50 could also be a separate device, such as a separate chip connected to microprocessor 44. Accounting module 52 may be EEPROM that incorporates ascending and descending registers as well as postal data, such as origination ZIP Code, vendor identification, data identifying the PC-based postage meter 10, sequential piece count of the postal revenue block generated by the PC-based postage meter 10, postage amount and the date of submission to the Postal Service. As is known, an ascending register in a metering unit records the amount of postage that has been dispensed, i.e., issued by the vault, in all transactions and the descending register records the value, i.e., amount of postage, remaining in the metering unit, which value decreases as postage is issued.

The hardware design of the vault includes an interface 56 that communicates with the host processor 22 through PCMCIA controller 32. Preferably, for added physical security, the components of vault 20 that perform the encryption and store the encryption keys (microprocessor 44, ROM 47 and NVM 46) are packaged in the same integrated circuit device/chip that is manufactured to be tamper proof. Such packaging ensures that the contents of NVM 46 may be read only by the encryption processor and are not accessible outside of the integrated circuit device. Alternatively, the entire card 30 could be manufactured to be tamper proof.

The memory of each NVM 46 is organized into sections. Each section contains historical data of previous transactions by vault 20. Examples of the types of transactions include: postage dispensed, tokens issued, refills, configuration parameters, and postal and vendor inspections. The size of each section depends on the number of transactions recorded and the data length of the type of transaction. Each section in turn is divided into transaction records. Within a section, the length of a transaction record is identical. The structure of a transaction record is such that the vault can check the integrity of data.

The functionality of DLL 40 is a key component of PC-base meter 10. DLL 40 includes both executable code and data storage area 41 that is resident in hard drive 24 of PC 12. In a Windows environment, a vast majority of applications programs 36, such as word processing and spreadsheet programs, communicate with one another using one or more dynamic link libraries. PC-base meter 10 encapsulates all the processes involved in metering, and provides an open interface to vault 20 from all Windows-based applications capable of using a dynamic link library. Any application program 36 can communicate with vault microprocessor 44 in PCMCIA card 30 through DLL 40.

DLL 40 includes the following software sub-modules. Secure communications sub-module 80 controls communications between PC 12 and vault 20. Transaction captures sub-module 82 stores transaction records in PC 12. Secure indicia image creation and storage sub-module 84 generates an indicia bitmap image and stores the image for subsequent printing. Application interface sub-module 86 interfaces with non-metering

application programs and issues requests for digital tokens in response to requests for indicia by the non-metering application programs. A more detailed description of PC meter system 10 and the generation of digital tokens is provided in previously noted U.S. Patent Applications Serial Nos. [Attorney Dockets E-421 and E-416] which are incorporated herein by reference.

Since printer 18 is not dedicated to the metering function, issued digital tokens may be requested, calculated and stored in PC 12 for use at a later time when, at a user's discretion, indicia corresponding to the issued digital tokens are generated and printed.

When PC-based meter system 10 is operating in a non-batch mode, a request for digital token is received from PC 12, vault 20 calculates and issues at least one digital token to PC 12 in response to the request. The issued digital token is stored as part of a transaction record in PC 12 for printing at a later time. In the preferred embodiment of the present invention, the transaction record is stored in a hidden file in DLL storage area 41 on hard drive 24. Each transaction record is indexed in the hidden file according to addressee information. It has been discovered that this method of issuing and storing digital tokens provides an additional benefit that one or more digital tokens can be reissued from DLL 40 rather than from vault 20 whenever a token has not been printed or if a problem has occurred preventing a printing of an indicia with the token.

By storing digital tokens as part of transaction records in PC 12 the digital tokens can be accessed at a later time for the generation and printing of indicia which is done in PC 12. Fig. 5 illustrates differences between conventional meter processing and delayed printing processing of the present invention.

The storage of transaction records that include vault status at the end of each transaction provides a backup to the vault with regard to accounting information as well as a record of issued tokens. The number of transaction records stored on hard drive 24 may be limited to a predetermined number, preferably including all transactions since the last refill of vault 20. In previously noted U.S. Patent Application Serial No. [Attorney Docket E-420], which is incorporated herein by reference, the method of backing up such transactions and recovery therefrom is described.

Referring now to Fig. 6, the preferred method of the present invention is shown. At step 200, a check is made to see if PC-based meter 10 is in batch mode. If not then the generation of digital tokens occurs, at step 202, as described in previously noted U.S. Patent Application Serial No. [Attorney Docket E-416]. If in batch mode, then, at step 204, the batch index i is set to zero. At step 206, a request for the ith indicia RI(i) is made. At step 208, the process waits for a digital token to be generated in response to the request. When the token, which is part of a transaction record, is received from vault 20, a check is made, at step 210, to determine if the entire batch of n tokens has been received from vault 20. If not, then, at step 212, index i is incremented and the process continues at step 206. If the batch is completed, then, at step 214, a second batch index i is set to zero. At step 216, a bit-mapped image of the ith indicia I(i) is generated from the corresponding transaction record. At step 218, the bit-mapped indicia image is combined with a fixed graphics image and the resulting ith indicia image is stored in DLL 40. At step 220, the ith transaction record TR(i) is stored in DLL storage file 41. Then, at step 230, a check is made to determine if all n indicia of the batch have been generated. If not, then at step 232, the index is incremented and the process continues at step 216.

Referring now to Fig. 7, an alternate method is shown in which a batch of digital tokens are issued in vault 20 before being sent to PC 12 as a batch of digital tokens. At step 240, a check is made to see if PC-based meter 10 is in batch mode. If not then the generation of digital tokens occurs, at step 242, as described in previously noted U.S. Patent Application Serial No. [Attorney Docket E-416]. If in batch mode, then, at step 244, vault 20 receives a request for a batch of digital tokens. At step 246, index i is set to zero. At step 248, vault 20 reads the postal data relating to the ith transaction requested and at step 250 calculates a digital token T(i) therefor. At step 252, vault 20 stores the transaction record TR(i) in the vault. A check is made, at step 254, to determine if the entire batch of n tokens has been issued by vault 20. If not, the index is incremented at step 256 and the process continues at step 248. If the batch has been completed, then, at step 258, the batch of transaction records are sent to PC 12 for storage and the generation of indicia corresponding to the batch of digital tokens in the transaction records.

While the present invention has been disclosed and described with reference to a single embodiment thereof, it will be apparent, as noted above that variations and modifications may be made therein. It is, thus, intended in the following claims to cover each variation and modification that falls within the true spirit and scope of the present invention.

In the foregoing, the following attorney docket references indicate the US-applications shown in the following table. All these applications have corresponding European Applications and are hereby incorporated herein by reference:

E-415	Serial No. 08/575,106
E-416	Serial No. 08/575,107
E-417	Serial No. 08/574,746
E-418	Serial No. 08/574,745
E-419	Serial No. 08/575,110
E-420	Serial No. 08/574,743
E-421	Serial No. 08/575,112
E-444	Serial No. 08/575,109
E-452	Serial No. 08/575,104
E-463	Serial No. 08/574,749
E-466	Serial No. 08/575,111
E-462	Serial No. 08/588,499

Claims

1. A transaction evidencing system, comprising:

   a host processor;
   unsecured printing means coupled to the host processor;
   vault means operatively coupled to said host processor, said vault means including digital token generation means and transaction accounting means, said digital token generation means generating a digital token in response to a first command from said host processor;
   storage means operatively coupled to at least one of said vault means and said host processor for storing said digital token and information relating thereto;
   means for selectively accessing said stored digital token and said information relating thereto and for generating transaction evidencing indicia corresponding to such stored digital token, said unsecured printing means printing said transaction evidencing indicia in response to a second command which is issued at a time subsequent to said first command.

2. The system of claim 1 wherein a batch of digital tokens may be generated and stored in an indexed file in said storage means before any indicia corresponding to said batch of digital tokens are generated and printed.

3. The system of claim 1 wherein the host processor is a personal computer and said vault means is a portable vault card that is removably coupled to the personal computer.

4. A method of printing an indicia separate from generating a digital token in an open metering system, the method comprising the steps of:

   calculating a digital token in response to a request for digital token;
   storing the digital token and information related thereto as a transaction record;
   accessing the stored digital token and the information related thereto at a later time when an indicia is to be generated and printed;
   generating the indicia;
   printing the indicia.

5. The method of claim 4 wherein the steps of calculating the digital token and storing the transaction record are repeated for each request in a batch of requests for digital token before each of the remaining steps is repeated sequentially for each digital token in the batch of digital tokens generated and stored.

6. The method of claim 5, wherein the step of storing each transaction record includes storing to an indexed file.

7. The method of claim 6, wherein said information related thereto is postal information including piece count, postage amount and addressee information and said indexed file is indexed according to addressee information.

8. The method of claim 4, comprising the further step of:

   viewing on a display an image of at least a part of a document with the indicia shown thereon before printing the document.

9. The system of claim 3 wherein said information related thereto is postal information including piece count, postage amount and addressee information and said indexed file is indexed according to addressee information.

FIG. 1

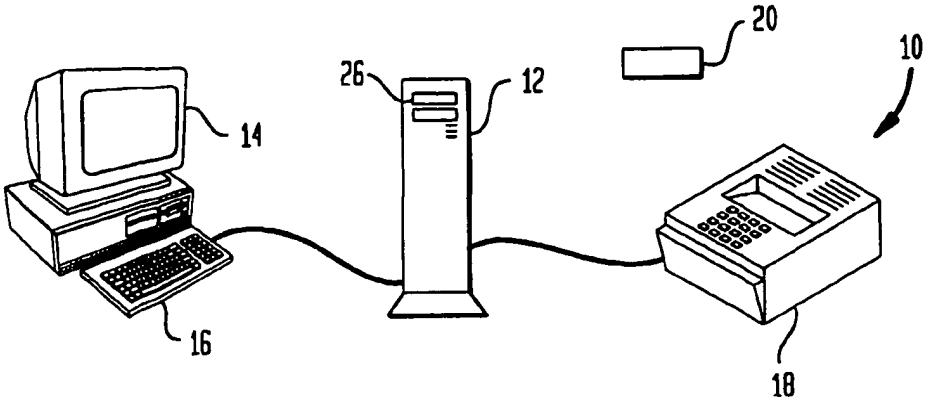

20
10
26
12
14
16
18

FIG. 2

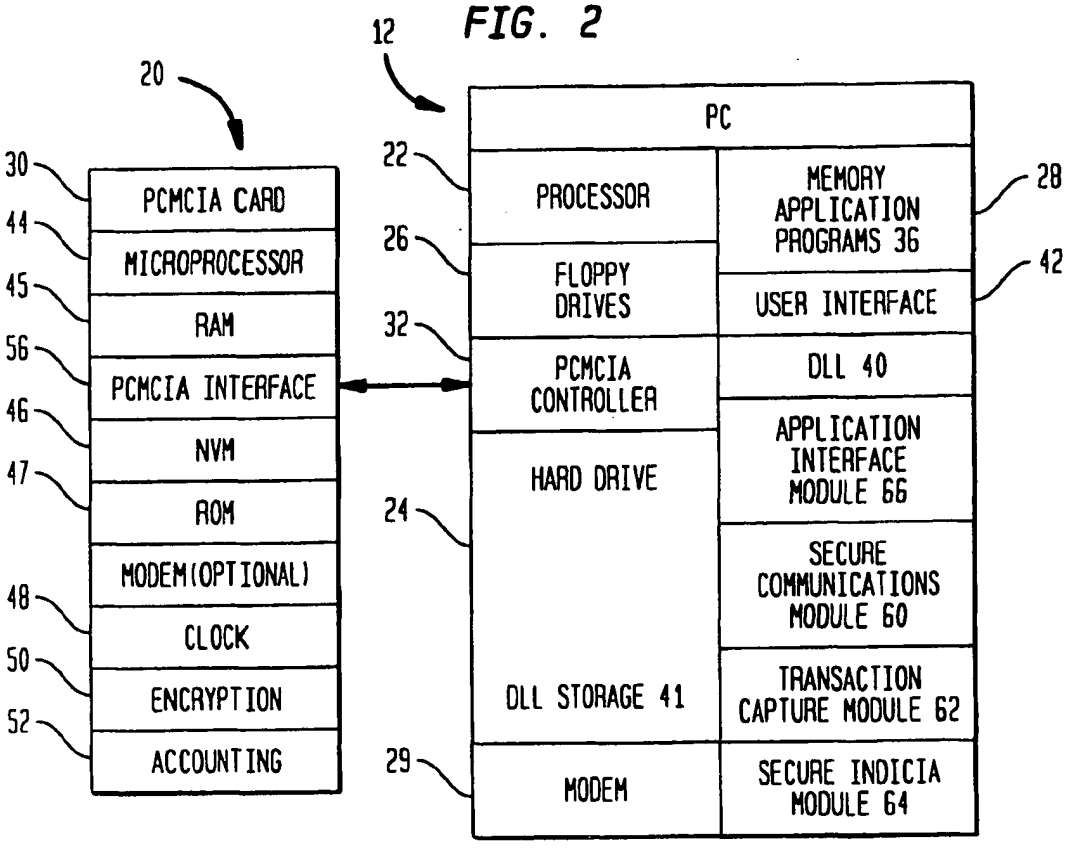

12
20
PC
30
PCMCIA CARD
44
MICROPROCESSOR
45
RAM
56
PCMCIA INTERFACE
46
NVM
47
ROM
MODEM(OPTIONAL)
48
CLOCK
50
ENCRYPTION
52
ACCOUNTING
22
PROCESSOR
26
FLOPPY DRIVES
32
PCMCIA CONTROLLER
HARD DRIVE
24
DLL STORAGE 41
29
MODEM
28
MEMORY APPLICATION PROGRAMS 36
42
USER INTERFACE
DLL 40
APPLICATION INTERFACE MODULE 66
SECURE COMMUNICATIONS MODULE 60
TRANSACTION CAPTURE MODULE 62
SECURE INDICIA MODULE 64

FIG. 3

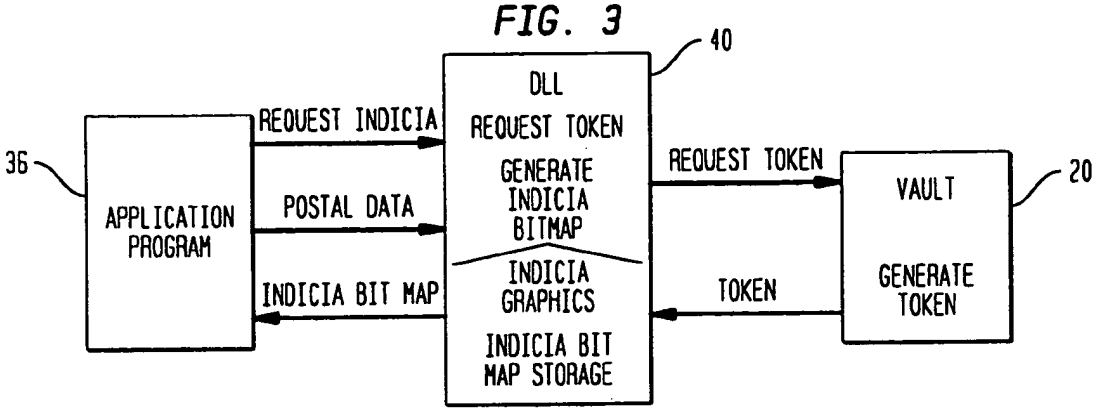

36
APPLICATION PROGRAM
REQUEST INDICIA
POSTAL DATA
INDICIA BIT MAP
DLL
REQUEST TOKEN
GENERATE INDICIA BITMAP
INDICIA GRAPHICS
INDICIA BIT MAP STORAGE
40
REQUEST TOKEN
TOKEN
VAULT
GENERATE TOKEN
20

FIG. 4

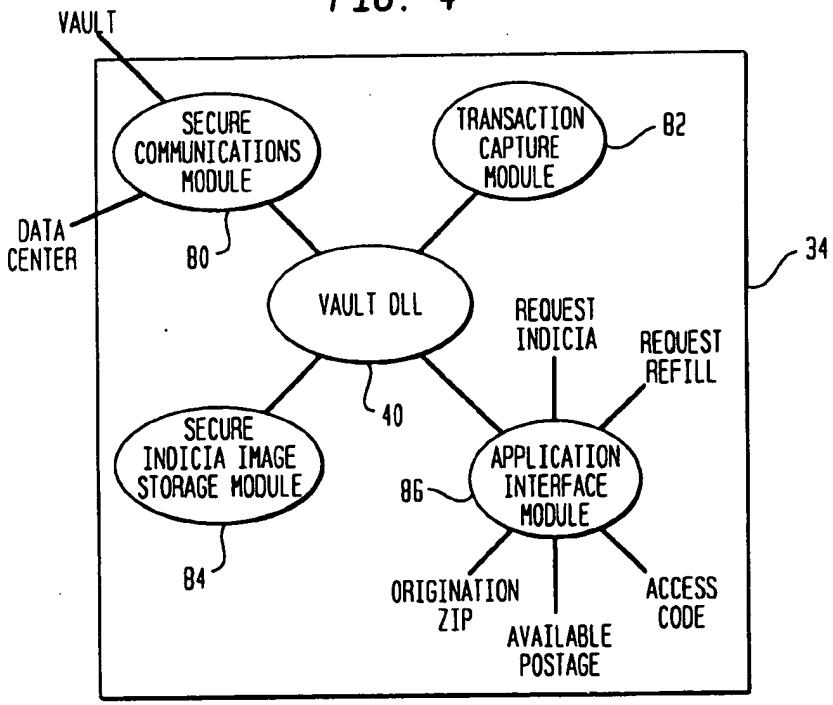

VAULT
SECURE COMMUNICATIONS MODULE
DATA CENTER
80
TRANSACTION CAPTURE MODULE
82
34
VAULT DLL
40
REQUEST INDICIA
REQUEST REFILL
SECURE INDICIA IMAGE STORAGE MODULE
84
APPLICATION INTERFACE MODULE
86
ORIGINATION ZIP
AVAILABLE POSTAGE
ACCESS CODE

FIG. 5

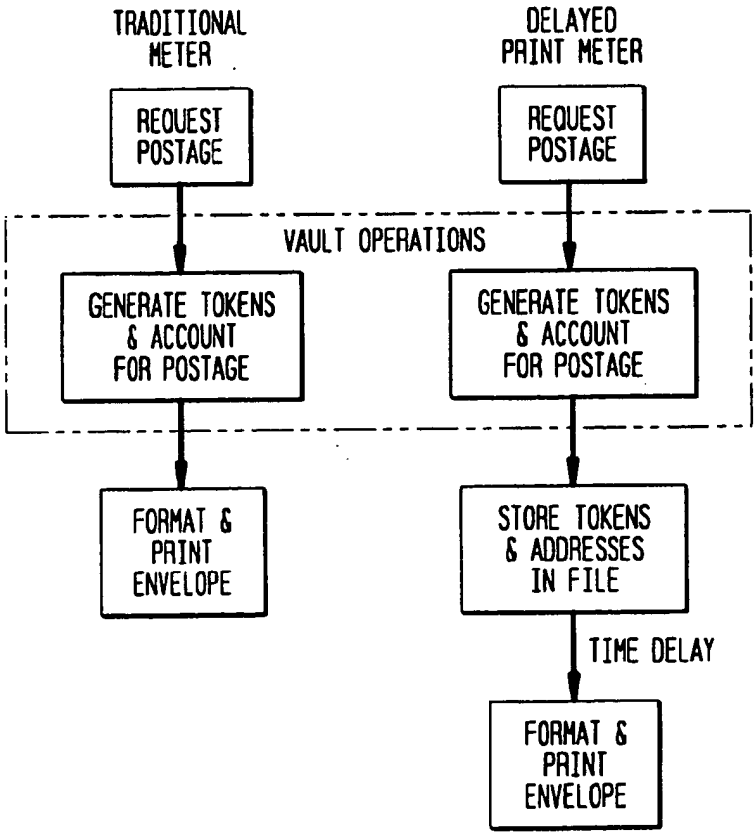

TRADITIONAL METER
DELAYED PRINT METER
REQUEST POSTAGE
REQUEST POSTAGE
VAULT OPERATIONS
GENERATE TOKENS & ACCOUNT FOR POSTAGE
GENERATE TOKENS & ACCOUNT FOR POSTAGE
FORMAT & PRINT ENVELOPE
STORE TOKENS & ADDRESSES IN FILE
TIME DELAY
FORMAT & PRINT ENVELOPE

FIG. 6

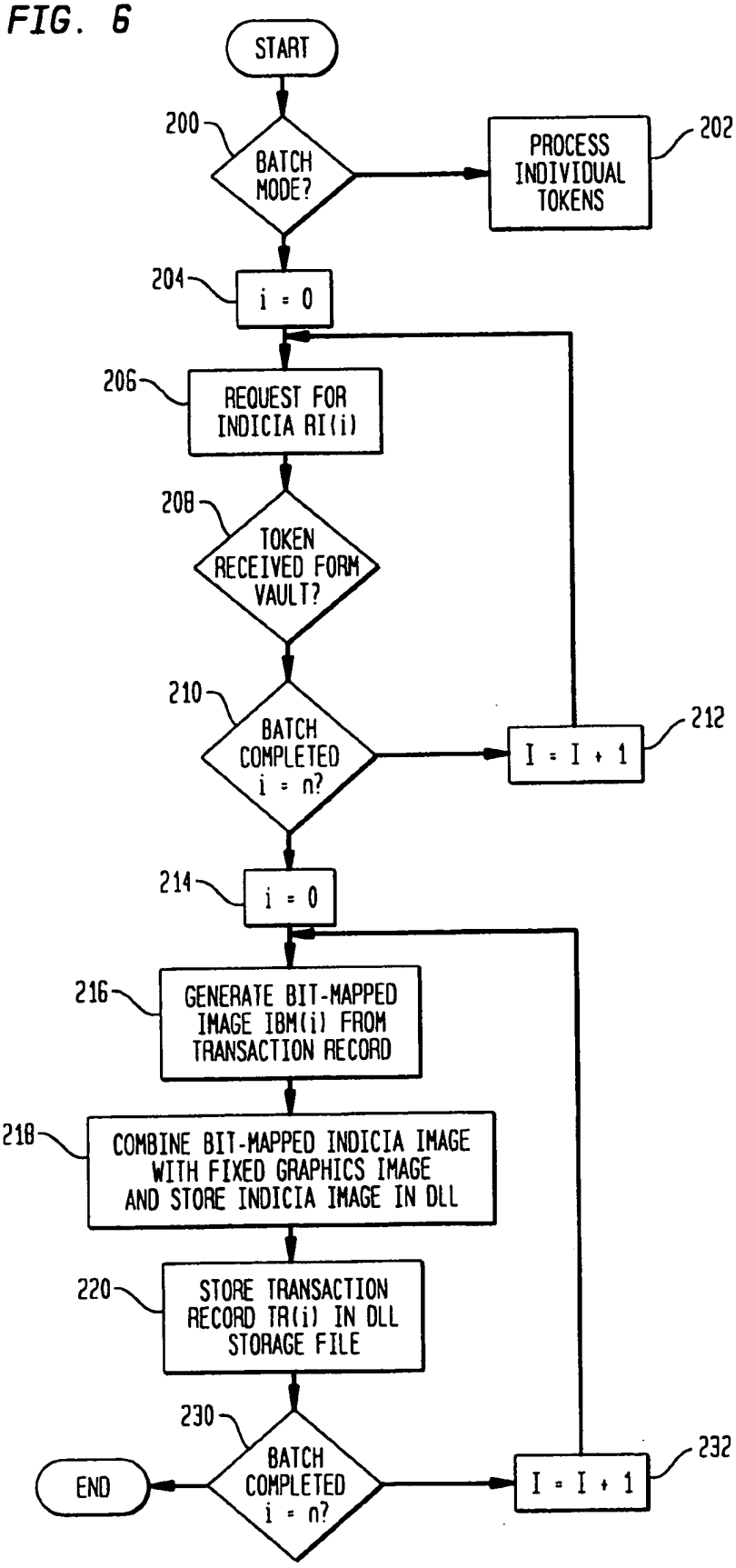
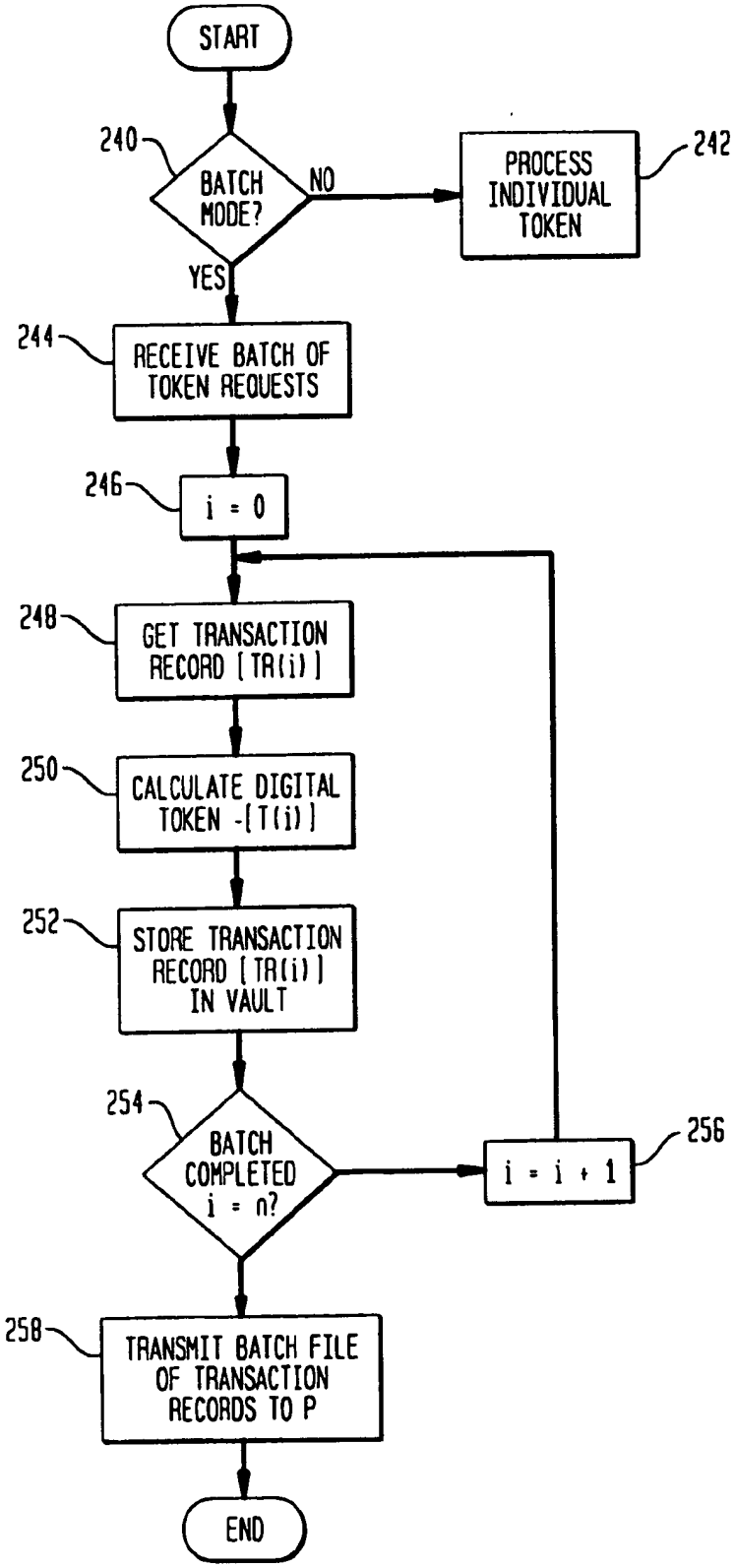

START
200
BATCH MODE?
PROCESS INDIVIDUAL TOKENS
202
204
i = 0
206
REQUEST FOR INDICIA RI(i)
208
TOKEN RECEIVED FORM VAULT?
210
BATCH COMPLETED i = n?
I = I + 1
212
214
i = 0
216
GENERATE BIT-MAPPED IMAGE IBM(i) FROM TRANSACTION RECORD
218
COMBINE BIT-MAPPED INDICIA IMAGE WITH FIXED GRAPHICS IMAGE AND STORE INDICIA IMAGE IN DLL
220
STORE TRANSACTION RECORD TR(i) IN DLL STORAGE FILE
230
BATCH COMPLETED i = n?
END
I = I + 1
232

FIG. 7


START
240
BATCH MODE?
NO
242
PROCESS INDIVIDUAL TOKEN
YES
244
RECEIVE BATCH OF TOKEN REQUESTS
246
i = 0
248
GET TRANSACTION RECORD [TR(i)]
250
CALCULATE DIGITAL TOKEN -[T(i)]
252
STORE TRANSACTION RECORD [TR(i)] IN VAULT
254
BATCH COMPLETED i = n?
256
i = i + 1
258
TRANSMIT BATCH FILE OF TRANSACTION RECORDS TO P
END